



July 21, 2009 12:15am AEST

No system is secure

Karen Dearne | July 21, 2009

NEW operating systems such as Google's planned Chrome and Microsoft's Windows 7 are only secure until they're released on the market, driving growth for software security vendors, according to McAfee chief executive Dave DeWalt.

"When operating systems are brand new, often they are viewed as very secure," Mr DeWalt said.

"But as they go into production and are installed in systems, vulnerabilities are discovered and the exploits begin.

"Certainly Microsoft, Red Hat and Apple can attest to that, and in our view it's just a matter of time before we see vulnerabilities exploited on a Chrome operating system as well."

Mr DeWalt said Google had the luxury of learning from previous developments, and as a result could be more secure, but "no operating system in the history of technology has been completely secure".

McAfee had partnered with Microsoft on Windows 7 as part of the software giant's outreach to the security sector, but as 7's release drew closer "the cybercrime eco-system will be looking for vulnerabilities".

"Microsoft has put concerted effort into building more secure platforms but despite that, the number of exploits has continued to grow," Mr DeWalt said.

"In the past 90 days, we've seen in excess of 40 critical vulnerability exploits on Microsoft and this is the highest rate we've ever seen.

"Zero-day attacks, Patch Tuesdays and the Conficker worm, which was a very large Microsoft exploit -- these are heavy threats."

Operating systems that allowed collaborative environments for building applications, such as Facebook, Twitter and eBay, created huge risks for security breaches, he said.

"Some of the biggest challenges here are due to simply not understanding what's coming next," he said. "Wherever you see the crowds, that's where you'll see new malware, and most of these exploits are financially motivated.

"Over the past 12 to 18 months, much of the malware has been deployed through social networking applications, and many have been deployed through mobile devices like new smartphones."

The recent Twitter worm -- created by a 17-year-old -- which caused a US shutdown of the site, downloaded a small keylogging program to capture credit card numbers and identity details that users entered into their computers.

Copyright 2009 News Limited. All times AEST (GMT +10).